

KATA PENGANTAR

Puji syukur kepada kehadiran Allah SWT, yang senantiasa melimpahkan rahmat dan hidayah-Nya sehingga dapat menyelesaikan penelitian yang berjudul “Perbandingan Kinerja Deteksi Aplikasi *Snort* dan *Suricata* Dalam Mengidentifikasi Serangan *Denial Of Service*” dengan sebaik-baiknya.

Penelitian ini merupakan salah satu syarat akademik bagi seluruh mahasiswa Jurusan Informatika Fakultas Teknik Universitas Siliwangi. Dalam penyusunan penelitian ini banyak sekali bantuan oleh berbagai pihak, baik langsung maupun tidak langsung.

Dalam penyusunan laporan ini banyak dibantu oleh berbagai pihak, baik langsung maupun tidak langsung. Untuk itu mengucapkan terima kasih sebesar-besarnya kepada :

1. Bapak Prof. Dr. Eng H. Aripin, selaku Dekan Fakultas Teknik Universitas Siliwangi Tasikmalaya
2. Bapak Nur Widiyasono, S.Kom., M.Kom. selaku Ketua Jurusan Informatika Universitas Siliwangi Tasikmalaya sekaligus pembimbing 2 yang telah membimbing dengan penuh kesabaran dan memberikan arahan serta saran dalam penyusunan laporan ini.
3. Bapak Rohmat Gunawan, S.T., M.T. selaku pembimbing 1 sekaligus Dosen Wali yang senantiasa sabar memberikan bimbingan, arahan, dan meluangkan waktu serta pikirannya dalam menyempurnakan laporan Tugas Akhir ini.

4. Rekan-rekan mahasiswa Universitas Siliwangi khususnya Informatika angkatan 2017.
5. Dan semua pihak yang tidak dapat disebutkan satu persatu yang telah memberi bantuan dan dorongan baik moril maupun materil.

Semoga laporan hasil Tugas Akhir ini dapat memberikan informasi yang bermanfaat bagi pembaca, tanpa melupakan banyaknya kekurangan yang ada dalam laporan. Maka dari itu dengan senang hati akan menerima kritik serta saran untuk perbaikan laporan ini. Terima kasih atas bantuannya dan semoga Allah SWT membalasnya.

Tasikmalaya, Maret 2021

Penulis

DAFTAR ISI

	Halaman
LEMBAR PENGESAHAN PEMBIMBING.....	i
LEMBAR PENGESAHAN PENGUJI	ii
LEMBAR PERNYATAAN KEASLIAN	iii
ABSTRACT.....	iv
ABSTRAK.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xiii
BAB I PENDAHULUAN	I-1
1.1. Latar Belakang.....	I-1
1.2. Rumusan Masalah	I-3
1.3. Tujuan Penelitian	I-4
1.4. Manfaat Penelitian.....	I-4
1.5. Ruang Lingkup Penelitian	I-4
1.6. Struktur Penulisan Penelitian	I-5
BAB II TINJAUAN PUSTAKA.....	II-1
2.1. <i>Denial of Service (DOS)</i>	II-1

2.1.1.	<i>Syn Flooding</i>	II-1
2.1.2.	<i>XMAS Flood</i>	II-2
2.1.3.	<i>Slowloris</i>	II-2
2.2.	<i>Intrusion Detection System (IDS)</i>	II-3
2.3.	<i>Intrusion Prevention System (IPS)</i>	II-4
2.4.	Penelitian Terkait.....	II-4
BAB III METODE PENELITIAN.....		III-1
3.1.	Metodologi Penelitian	III-1
3.2.	Analisis Sistem	III-2
3.3.	Identifikasi Kebutuhan Hardware dan Software	III-2
3.4.	Perancangan Arsitektur Sistem.....	III-3
3.5.	Implementasi dan Pengujian.....	III-3
3.6.	Pengukuran Hasil Pengujian.....	III-6
BAB IV HASIL DAN PEMBAHASAN		IV-1
4.1.	Implementasi	IV-1
4.2.	Pengujian	IV-3
4.2.1.	<i>TCP Syn Flooding</i>	IV-5
4.2.2.	<i>TCP XMAS Flooding</i>	IV-10
4.2.3.	<i>Slowloris Attack</i>	IV-15
4.3.	Data Hasil Pengujian	IV-20

4.3.1.	Perbandingan Total Deteksi	IV-20
4.3.2.	Perbandingan Penggunaan CPU.....	IV-25
4.3.3.	Perbandingan Penggunaan Memori	IV-29
4.3.4.	Perbandingan <i>Load Average</i>	IV-33
4.4.	Perbandingan Aplikasi.....	IV-38
BAB V PENUTUP.....		V-1
5.1.	Kesimpulan	V-1
5.2.	Saran	V-2

REFERENSI

DAFTAR TABEL

Tabel 2.1 Penelitian terkait (State of the art)	II-4
Tabel 3.1 Spesifikasi hardware yang digunakan	III-2
Tabel 3.2 Pembagian spesifikasi virtualisasi	III-2
Tabel 3.3 Spesifikasi software yang digunakan	III-2
Tabel 3.4 Skenario pengujian	III-4
Tabel 4.1 Hasil deteksi aplikasi snort.....	IV-3
Tabel 4.2 Hasil deteksi suricata.....	IV-4
Tabel 4.3 Data pengujian syn flooding snort	IV-6
Tabel 4.4 Load average serangan syn flooding pada snort	IV-7
Tabel 4.5 Total deteksi, penggunaan cpu dan ram suricata	IV-8
Tabel 4.6 Load average suricata pada serangan syn flooding	IV-9
Tabel 4.7 Data deteksi, cpu usage, memori usage xmas snort	IV-11
Tabel 4.8 Load average serangan xmas snort	IV-12
Tabel 4.9 Data deteksi, penggunaan cpu dan memori xmas suricata.....	IV-13
Tabel 4.10 Load average serangan xmas flood suricata.....	IV-14
Tabel 4.11 Data deteksi, cpu usage, memori usage serangan slowloris snort..	IV-16
Tabel 4.12 Load average serangan slowloris snort	IV-17
Tabel 4.13 Deteksi, penggunaan cpu dan memori slowloris suricata	IV-19
Tabel 4.14 Load average serangan slowloris suricata.....	IV-20
Tabel 4.15 Perbandingan total deteksi serangan syn flooding	IV-21
Tabel 4.16 Perbandingan deteksi serangan XMAS Flood	IV-22
Tabel 4.17 Perbandingan deteksi serangan slowloris.....	IV-23

Tabel 4.18 Perbandingan penggunaan cpu serangan syn flooding	IV-25
Tabel 4.19 Perbandingan penggunaan cpu serangan xmas flood.....	IV-26
Tabel 4.20 Perbandingan penggunaan cpu serangan slowloris	IV-27
Tabel 4.21 Perbandingan penggunaan memori serangan syn flooding.....	IV-29
Tabel 4.22 Perbandingan penggunaan memori serangan xmas flood	IV-30
Tabel 4.23 Perbandingan penggunaan memori serangan slowloris	IV-31
Tabel 4.24 Perbandingan load average serangan syn flooding	IV-33
Tabel 4.25 Perbandingan load average serangan xmas flood	IV-34
Tabel 4.26 Perbandingan load average serangan slowloris	IV-37
Tabel 4.27 Perbandingan deteksi, penggunaan cpu, dan memori aplikasi.....	IV-39
Tabel 4.28. Perbandingan load average setiap serangan DOS	IV-40

DAFTAR GAMBAR

Gambar 2.1 Koneksi TCP ke Server	II-1
Gambar 2.2 Alur deteksi IDS.....	II-3
Gambar 3.1 Tahapan penelitian	III-1
Gambar 3.2 Skema Jaringan Penelitian.....	III-3
Gambar 3.3 Contoh total paket terkirim serangan syn flood	III-5
Gambar 3.4 Contoh total paket terkirim serangan xmas flood	III-5
Gambar 3.5 Contoh total koneksi terbuka serangan slowloris.....	III-6
Gambar 4.1 Interfaces snort	IV-2
Gambar 4.2 Interfaces Suricata	IV-2
Gambar 4.3 Alert serangan syn flood aplikasi snort	IV-5
Gambar 4.4 Data cpu usage, memori usage dan load average snort	IV-6
Gambar 4.5 Alert serangan syn flooding aplikasi suricata.....	IV-7
Gambar 4.6 Penggunaan cpu, memori, dan load average suricata.....	IV-8
Gambar 4.7 Deteksi xmas flood aplikasi snort	IV-10
Gambar 4.8 Penggunaan cpu, memori dan load average snort serangan xmas	IV-11
Gambar 4.9 Deteksi serangan xmas flood suricata	IV-12
Gambar 4.10 Penggunaan cpu, memori dan load average suricata xmas	IV-13
Gambar 4.11 Deteksi serangan slowloris snort	IV-15
Gambar 4.12 Data cpu, memori, dan load average snort serangan slowloris ..	IV-16
Gambar 4.13 Deteksi serangan slowloris suricata	IV-18
Gambar 4.14 Data cpu, memori, dan load average suricata slowloris	IV-19
Gambar 4.15 Grafik perbandingan deteksi syn flooding	IV-21

Gambar 4.16 Grafik deteksi serangan xmas flood	IV-23
Gambar 4.17 Grafik deteksi serangan slowloris	IV-24
Gambar 4.18 Grafik penggunaan cpu serangan syn flooding	IV-25
Gambar 4.19 Grafik penggunaan cpu serangan xmas flood	IV-27
Gambar 4.20 Grafik penggunaan cpu serangan slowloris.....	IV-28
Gambar 4.21 Grafik penggunaan memori serangan syn flooding	IV-29
Gambar 4.22 Grafik penggunaan memori serangan xmas flood.....	IV-31
Gambar 4.23 Grafik penggunaan memori serangan slowloris.....	IV-32
Gambar 4.24 Grafik load average aplikasi snort pada serangan syn flooding .	IV-34
Gambar 4.25 Grafik load average aplikasi suricata pada syn flooding.....	IV-34
Gambar 4.26 Grafik load average snort terhadap serangan xmas flood	IV-35
Gambar 4.27 Grafik load average suricata terhadap serangan xmas flood	IV-36
Gambar 4.28 Grafik load average snort terhadap serangan slowloris.....	IV-37
Gambar 4.29 Grafik load average suricata terhadap serangan slowloris	IV-38
Gambar 4.30 Grafik perbandingan aplikasi	IV-39
Gambar 4.31 Grafik perbandingan load average setiap serangan	IV-40